UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,938	01/12/2004	Simon Robert Walmsley	PEA26US	7678

24011 7590 10/31/2008
SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
10/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/754,938	**Applicant(s)** WALMSLEY, SIMON ROBERT	
	Examiner DEVIN ALMEIDA	**Art Unit** 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 7/03/2008.

Response to Arguments

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 4-7, 17, 18 and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Raivisto (U.S. Patent # 6,081,601).

With respect to claim 1, a method of passing validated information along a series of entities, the series of entities including a source entity, at least one intermediate entity, and a target entity, wherein each of the entities shares a validation parameter with its immediately neighboring entity or entities in the series, the method comprising the steps, commencing in the source entity, of: (a) in the source entity, generating a validation code for the information (secret key encrypted message), the validation code being based on the validation parameter (see figure 4A i.e. the secret key) shared between the current entity and a next entity in the series (see column 4 line 54 – column

5 line 14 i.e. secret key shared between MS1 and the mediator MD); (b) outputting the validation code (see column 4 line 54 – column 5 line 14 i.e. MS1 transmits the encrypted message 81, which is then routed via the GSM network to the short message service center SMSC according to prior art. There is no need to decrypt the message for routing, since the address of the receiving party is not encrypted. According to the invention, the SMSC recognizes the message and forwards it to a mediator MD); (c) receiving the validation code in the next entity (mediator) in the series and making that entity the current entity (see column 4 line 54 – column 5 line 14 i.e. MS1 transmits the encrypted message 81, which is then routed via the GSM network to the short message service center SMSC according to prior art. There is no need to decrypt the message for routing, since the address of the receiving party is not encrypted. According to the invention, the SMSC recognizes the message and forwards it to a mediator MD); (d) verifying the information via the validation code in the current entity using the validation parameter required to verify it (see column 4 line 54 – column 5 line 14 mediator MD which decrypts the message); (e) in the current entity (mediator MD), generating a validation code for the information (secret key encrypted message), the validation code being based on the validation parameter (see figure 4A i.e. the secret key) shared between the current entity and a next entity in the series (see column 4 line 54 – column 5 line 14 i.e. secret key shared between MS2 and the mediator MD); (f) outputting the validation code (see column 4 line 54 – column 5 line 14 i.e. mediator MD then transfers the re-encrypted cipher text back to the SMSC (transfer 85). If the SMSC is the mediator, transfers 83 and 85 are not needed. The SMSC forwards the cipher text to the

receiving party MS2); (h) verifying the information via the validation code in the current entity using the validation parameter required to verify it (see column 4 line 54 – column 5 line 14); and (j) repeating steps (e) to (h) until the current entity in step (g) and (h) is the target entity (MS2 is target entity).

With respect to claim 2 wherein step (b) includes the substep of outputting the information (see column 4 line 54 – column 5 line 14 i.e. MS1 transmits the encrypted message 81).

With respect to claim 4, wherein step (c) includes receiving the information and using it during the verification (see column 4 line 54 – column 5 line 14 i.e. MS1 transmits the encrypted message 81, which is then routed via the GSM network to the short message service center SMSC according to prior art. There is no need to decrypt the message for routing, since the address of the receiving party is not encrypted. According to the invention, the SMSC recognizes the message and forwards it to a mediator MD).

With respect to claim 5, further including a controller in contact with at least some of the entities, the controller being configured to pass the information and/or the validation codes between adjacent entities in the series (see column 4 line 54 – column 5 line 29 i.e. mediator).

With respect to claim 6, wherein step (a) is performed in response to an instruction issued by the controller (see column 4 line 54 – column 5 line 29).

With respect to claim 7, wherein the instruction includes a request for the information upon which the validation is to be performed (see column 4 line 54 – column 5 line 29).

With respect to claim 17, wherein a different validation parameter is used for the validation step performed at any two adjacent entities (see column 4 line 54 – column 5 line 29 i.e. secret key shared between MS1 and the mediator MD and secret key shared between MS2 and the mediator MD).

With respect to claim 18, wherein at least one of the entities is an integrated circuit (see column 4 line 54 – column 5 line 29).

With respect to claim 23, where one of the entities is the controller (see column 4 line 54 – column 5 line 29 i.e. mediator).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raivisto (U.S. Patent # 6,081,601) in view of Schneier <u>Applied Cryptography Protocols, Algorithms and Source Code in C</u>.

With respect to claim 8 Wiegley teaches everything with respect to claim 1 above but does not teach wherein the validation code is a digital signature produced by a digital signature function using the information and the validation parameter as operands. Schneier teaches that the validation code is a digital signature produced by a digital signature function using the information and the validation parameter as operands (see Schneier page 37-38). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have digital signed the information with the senders private key. This makes it so the receiver can verify who sent the information by decrypting the information with the sender's public key (see Schneier page 37-38). Therefore one would be motivated to have digital signed the information.

With respect to claim 9, wherein the validation parameter is a key (see figure 4A i.e. the session key and the public key of the printer).

With respect to claim 10, wherein the key is a symmetric key (see figure 4A i.e. the session key and the public key of the printer).

With respect to claim 11, wherein the validation parameter is an asymmetric key-pair, and the public and private components of the key-pair are in respective neighboring entities in the series (see figure 4A i.e. the session key and the public key of the printer).

With respect to claim 12, wherein the validation code is a digital signature (see Schneier page 37-38) generated with a digital signature function using the key or key-pair component (see figure 4A i.e. the session key), the information (see figure 4A i.e. the print data) and at least one nonce as inputs (see figure 4A i.e. the session key).

With respect to claim 13, wherein the at least one nonce is generated in the current entity in response to an instruction issued by the neighboring entity of the current entity closer to the target entity (see figure 4A i.e. the session key).

With respect to claim 14, wherein the at least one nonce is randomly, pseudo-randomly or arbitrarily generated number (see figure 4A i.e. the session key and column 4 lines 47-52).

With respect to claim 15, wherein the at least one nonce is supplied to the current entity in an instruction issued by the neighbouring entity of the current entity closer to the target entity (see figure 4A i.e. the session key).

With respect to claim 16, wherein the nonce is randomly, pseudo-randomly or arbitrarily generated number (see figure 4A i.e. the session key and column 4 lines 47-52).

Claims 19-22, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raivisto (U.S. Patent # 6,081,601) in view of Wiegley (U.S. Patent # 6,711,677).

Raivisto does not teach with respect to claim 19, wherein the target entity and the source entity, and is a printer controller integrated circuit. Wiegley teaches wherein the target entity and the source entity is a printer controller integrated circuit (see Wiegley figure 2 element 22 and column 3 lines 41-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the system of Raivisto in transferring data from one device to another device in the system of Wiegley to allow the Wiegley invention to transfer message between the personal computer and printer without the printer needing to store a secret key with every computer that is connecter to the network. MS1 (the personal computer) and MS2 (the Printer) only need to know the cryptographic parameters of the mediator MD to send messages to the printer, not the cryptographic parameters of each other, since the mediator MD alone handles the end user's security parameters (see Raivisto column 5 lines 16-29). Therefore one would be motivated to have used the system of Raivisto in transferring data from one device to another device in the system of Wiegley as an easy way for the printer to receive secure document from all the connected computers.

With respect to claim 19. A method according to claim 1, wherein the target entity is a printer controller integrated circuit (see Wiegley figure 2 element 22 and column 3 lines 41-61).

With respect to claim 20, wherein the source entity is a printer controller integrated circuit (see Wiegley figure 2 element 18 and 20 and column 3 lines 41-61).

With respect to claim 21, wherein either the source entity (see Wiegley figure 2 element 12 personal computer) or the target entity (see Wiegley figure 2 element 10 i.e. printer) is a printer controller integrated circuit (see Wiegley figure 2 element 18, 20 and 22 and column 3 lines 41-61) and the at least one intermediate entity is a verification chip associated with the printer controller (see Wiegley figure 2 element 20 and column 3 lines 41-61).

With respect to claim 22, wherein the controller is a printer controller integrated circuit (see Wiegley figure 2 column 3 lines 41-61).

With respect to claim 24, wherein the printer controller has a relatively unique identity and the verification chip includes a key based on the unique identity (see Wiegley figure 4A and 4B the private key of the printer).

With respect to claim 25, wherein the source or target entity is an integrated circuit associated with a package that contains ink (see Wiegley figure 2 element 20 and figure 4B column 3 lines 41-61).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432